UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/833,342 | 04/12/2001 | David John Craft | AUS920010088US1 | 3785 |

45992 7590 10/24/2008

IBM CORPORATION (JVM)
C/O LAW OFFICE OF JACK V. MUSGROVE
2911 BRIONA WOOD LANE
CEDAR PARK, TX 78613

| EXAMINER | |
|---|---|
| PICH, PONNOREAY | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2435 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 10/24/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>09/833,342 | **Applicant(s)**<br>CRAFT ET AL. | |
| | **Examiner**<br>PONNOREAY PICH | **Art Unit**<br>2435 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *18 August 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *10-12,25 and 26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-12,25 and 26* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

Applicant's election of claims 10-12 and 25-26 for prosecution is noted. Claims 10-12 and 25-26 were examined.

### *Response to Amendment and Arguments*

Applicant's amendments to elected claims 10-12 and 25-26 submitted on 6/9/08 were noted. New rejections made below are made in response to the amendments and were necessitated by an updated search of the claims with the new limitations added.

Applicant's remarks were also noted. Applicant's summary of the interview held on 4/1/08 appears to be correct. The examiner notes that we had discussed features from the specification that the examiner thought had the best chance of getting the claims allowed at the time based on what the examiner had seen in searching thus far. Applicant is respectfully urged to thoroughly review the newly cited Shaw reference (US 6,381,741) found in an updated search and cited with this Office action. The examiner believes that this reference discloses several features that are also disclosed on page 23 of applicant's specification which the examiner had previously though had the best chance of gaining allowance for the case, including features found on page 23 not currently claimed. That this reference could not have been found earlier is regretted.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530) in further view of Epstein et al (US 6,694,025) in further view of Rose (US 5,708,709) and further in view of Shaw (US 6,381,741).

**Claim 10:**

As per claim 10, Arnold discloses the following limitations were well known in the art at the time applicant's invention was made:

1. Generating a client message at the client (col 2, lines 9-24).
2. Retrieving an embedded server public key from a memory structure in an article of manufacture (col 2, lines 9-24).
3. Encrypting the client message with the embedded server public key (col 2, lines 9-24).
4. Sending the client message to the server (col 2, lines 9-24).

Arnold does not explicitly disclose that in the prior art he discusses, the memory structure is read-only memory. Arnold also does not explicitly disclose the article of manufacture is in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship, the embedded client private key being associated with a client public key generated and stored exclusively outside the client.

However, Arnold discloses read-only memory being used to store keys (col 4, lines 14-17). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify the prior art teachings disclosed by Arnold so that the memory structure used to store keys was read-only memory structure. One skilled would have been motivated to do so because one skilled would appreciate that utilizing read-only memory to store keys would allow key information to be retained even if the device containing the memory were to lose power. One skilled would also be motivated to do so because use of read-only memory to store the keys prevents tampering with information stored in the memory, thus providing better security (Arnold: col 4, lines 36-40).

Further, Aoki discloses the article of manufacture is in the client, the memory structure having an embedded client private key, the embedded server public key and the embedded client key not being related by a public private key pair relationship, the embedded client private key being associated with a client public key stored exclusively outside the client (Fig 1, item 200). Note that in the figure cited, the client has stored in memory, the client's private key (i.e. individual private key) and a server's public key, but no client public key. As the client does not store the client's public key, the client's public key is stored exclusively outside the client. The private key of the client and the server's public key are not related by a public/private key pair relationship as they do not have an inverse relationship with one-another, i.e. plaintext encrypted by one cannot be decrypted by the other.

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify the client/server system disclosed by Aoki to use the secure communication techniques taught by Arnold (what he reveals was known in the prior art as well as what his own invention uses). One skilled would have been motivated to do so because it would allow Aoki's network system to establish a private and secure link between the clients and server of his invention for secure communication (Arnold: col 2, lines 23-24 and 43-44).

Aoki also does not explicitly disclose that the client's public key was generated exclusively outside the client. However, Epstein discloses that it was well known in the prior art to generate public/private key pairs exclusively outside the client, i.e. via a key generation server (col 2, lines 31-39; col 3, line 62-col 4, line 3; and col 4, lines 11-24). At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify the combination invention of Arnold and Aoki such that the client's public key was generated exclusively outside the client. One skilled would have been motivated to do so because as discussed by Epstein, the generation of a public/private key pair requires significant computational resources and generating the key pair outside the client would avoid the cost and loss of control that may result by enabling each user/client in a network environment to create the key pair (col 2, lines 31-39).

Arnold, Aoki, and Epstein do not explicitly disclose receiving a server message including application code from the server at the client in response to the client message, the application code having a first portion encrypted with a server private key and a second portion; and authenticating the first portion of the application code with the embedded server public key.

However, Rose discloses receiving a server message including application code from the server at the client in response to the client message, the application code having a first portion encrypted with a server private key and a second portion (Fig 4; col 3, lines 50-53; and col 5, lines 44-47). Figure 4 shows the format of an application code that is transmitted to the client in response to the client's request for the code. As seen in the Figure, the application code is composed of several portions. The first portion, item 182, is encrypted using the server's private key and the rest is considered the claimed second portion. Rose further discloses authenticating the first portion of the application code with the server public key (col 8, lines 15-31 and col 10, lines 4-29). Since the first portion of the application code seen in Figure 4 is encrypted using the server's private key, the server's public key is used to decrypt portion 182. The control information contained therein is authenticated as discussed in cited columns 8 and 10.

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Arnold, Aoki, and Epstein's combination invention using Rose's teachings such that the client's message is used to request an application code from a server and in response to the request, an application code in the format recited in claim 10 is sent back to the client and the sent application code was authenticated using the embedded server public key. Arnold’s prior art, Arnold, Aoki, Epstein, and Rose are all concerned with secure communication between a client and a server using asymmetric cryptographic techniques, thus the incorporation of Rose's teachings within the combination invention of Arnold, Aoki, and Epstein in the manner discussed would be nothing more than use of a known technique to improve similar devices (methods or products) in the same way. As per KSR v. Teleflex 550 U.S. ___, 127 S. Ct. 1727 (2007), this makes the invention as claimed obvious and unpatentable.

Arnold, Aoki, Epstein, and Rose do not explicitly disclose wherein the first portion of the application code is small relative to the second portion of the application code; and authenticating the second portion of the application code using an integrity checking algorithm that is not a public key algorithm. However, Shaw discloses of an application code downloaded from a server wherein the first portion of the application code is small relative to the second portion of the application code; and authenticating the second portion of the application code using an integrity checking algorithm that is not a public key algorithm (col 3, lines 40-44; col 4, lines 7-30; and col 5, lines 15-55). Note that the portions of Shaw cited discloses of a downloaded application code having a second portion used to check the integrity of the downloaded code by comparing a generated code with the second portion attached to the downloaded code. This second portion's validity is checked using either a MD5 algorithm or SHA1 algorithm, which one skilled in the art would understand generates an output smaller than the input. The integrity of the downloaded application is verified if the first portion is equal to the output generated by the client using the MD5 algorithm or SHA1 algorithm on the second portion. Note that both MD5 and SHA1 are not public key algorithms.

At the time applicant's invention was made, it would have been obvious to further modify the combination invention of Arnold, Aoki, Epstein, and Rose such that the application code has a first portion that is small relative to the second portion and authenticating the second portion of the application code using an integrity checking algorithm that is not a public key algorithm, i.e. by using MD5 or SHA1, as per Shaw's teachings. One skilled would have been motivated to do so because by providing an improved method of secure downloading which includes data integrity tests, it would solve a known problem in the prior art of client-server communication (col 1, lines 21-63).

Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530) in further view of Epstein et al (US 6,694,025) in further view of Rose (US 5,708,709) in further view of Shaw (US 6,381,741) and in further view of Sandhu et al (US 2002/0078344).

**Claim 11:**

As per claims 11, the combination of Arnold and Aoki discloses embedded client private key in a memory structure in an article of manufacture in the client (Aoki: Fig 1, item 200); the memory structure being read-only memory (Arnold: col 4, lines 14-17); and retrieving the client private key from the client's memory (Arnold: col 2, lines 25-41).

Arnold, Aoki, Epstein, and Rose do not explicitly disclose retrieving client authentication data; encrypting the client authentication data with the embedded client private key; and storing the encrypted client authentication data in the client message. However, these limitations are disclosed by Sandhu (paragraph 28).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify the combination invention of Arnold, Aoki, Epstein, Rose, and Shaw according to the limitations recited in claim 11 in light of Sandhu's teachings. One skilled would have been motivated to do so because it would provide client-side authentication (Sandhu: paragraph 28), thus making communication between the client and server more secure. Note that Arnold discusses authentication being desired objective for secure communication since before the time of his invention (col 2, lines 43-48).

Claims 12 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530) in further view of Epstein et al (US 6,694,025) in further view of Rose (US 5,708,709) in further view of Shaw (US 6,381,741) in further view of Sandhu et al (US 2002/0078344) and in further view of Davis (US 5,970,147).

**Claim 12:**

As per claim 12, Arnold, Aoki, Epstein, Rose and Sandhu do not explicitly disclose retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client; and storing a copy of the embedded client serial number in the client message. However, these limitations are disclosed by Davis (col 4, lines 26-39; col 5, lines 58-62; and col 6, lines 27-29).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify the combination invention of Arnold, Aoki, Epstein, Rose, Shaw, and Sandhu according to the limitations recited in claim 12. One skilled would have been motivated to do so because the client sending the serial number to the server alone with its message would allow the server to index various clients' public keys to the client's serial number, thus providing for a way for the server to look up the client key needed to authenticate the client's message.

**Claim 25:**

As per claim 25, the limitations recited therein are directed towards the server receiving and processing the message sent using the method of claim 12. One skilled would appreciate that a message sent by a client according to the limitations recited in claim 12 would be processed by the server according to the limitations recited in claims 25, thus the rejection for claim 25 flows from the rejection of claims 12.

**Claim 26:**

As per claim 26, the limitations recited therein are directed towards the server processing the authentication data sent by the client using a method having further limitations as recited in claim 11. One skilled would appreciate that a message sent by a client according to the further limitations recited in claim 11 would be processed by the server according to the limitations further recited in claim 26, thus the rejection for claim 26 flows from the rejections of claims 11 and 12.

## ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Examiner, Art Unit 2435